



RDR Corporate Accountability Index:

Transparency and accountability standards for
targeted advertising and algorithmic systems

PILOT STUDY AND LESSONS LEARNED

March 16, 2020

This work is licensed under the Creative Commons Attribution 4.0 International License.
To view a copy of this license, visit <https://creativecommons.org/licenses/by/4.0/>.



Acknowledgments

The following Ranking Digital Rights (RDR) team members were involved in conducting the research presented in this study and in drafting this report:

- Amy Brouillette, Research Director
- Nathalie Maréchal, Senior Policy Analyst
- Afef Abrougui, Research Analyst
- Zak Rogoff, Research Analyst
- Jan Rydzak, Company Engagement Lead and Research Analyst
- Veszna Wessenauer, Research Analyst
- Jie Zhang, Research Analyst
- Andrea Hackl, Research Fellow

We wish to thank the more than 90 experts who contributed valuable feedback on the draft indicators that were pilot tested in this study.

We also wish to thank the Open Society Foundations (OSF) for their generous support for our work and research in developing draft indicators presented in this report.

For a full list of project funders and partners:
<https://rankingdigitalrights.org/who/partners/>.

About Ranking Digital Rights

Ranking Digital Rights is a non-profit research initiative housed at the New America Foundation's Open Technology Institute. We work to promote freedom of expression and privacy on the internet by creating global standards and incentives for companies to respect and protect users' rights. We do this by ranking the world's most powerful digital platforms and telecommunications companies on relevant commitments and policies, based on international human rights standards. We work with companies as well as advocates, researchers, investors, and policymakers to establish and advance global standards for corporate accountability.

For more about our vision, impact, and strategy: www.rankingdigitalrights.org/about/.

For more about the RDR Corporate Accountability Index: www.rankingdigitalrights.org.

For more about the Open Technology Institute: <https://www.newamerica.org/oti/>.

For more about New America: <https://www.newamerica.org/>.

Contents

1. Introduction	4
1.1 About this pilot study	4
1.2 Why we are adding new indicators	5
1.3 Stakeholder engagement process	6
1.4 Next steps	6
2. Pilot study: Background and overview	7
2.1 Goals	7
2.2 Company selection	7
2.3 Research steps	8
2.4 Company evaluation and results	8
3. Summary of findings	10
4. Governance	13
4.1 Policy commitment	13
4.2 Human rights due diligence	15
5. Freedom of expression and information	19
5.1 Ad content policies and enforcement	21
5.2 Ad targeting policies and enforcement	23
5.3 Algorithmic system use policies	27
5.4 Algorithmic content curation	29
5.5 Bot policies	32
5.6 Informing and educating users about risks	34
6. Privacy	36
6.1 Algorithmic system development policies	38
6.2 Data inference policies	40
6.3 User control	42
6.4 Collection of user information by non-technical means	44
6.5 Inform and educate users about risks	45
6.6 User access to advertising targeting metadata	47
7. Most challenging indicators and issues	49
7.1 Algorithmic system use and development policies	49
7.2 Bot policies	49
7.3 Access to advertising metadata	50
8. Conclusions and next steps	51
9. Glossary of terms	52

1. Introduction

[Ranking Digital Rights](#) (RDR) works to promote freedom of expression and privacy on the internet by creating global standards and incentives for companies to respect and protect users' rights. We do this by producing the Ranking Digital Rights Corporate Accountability Index, which evaluates the world's most powerful digital platforms and telecommunications companies on relevant commitments and policies, based on international human rights standards. We work with companies as well as advocates, researchers, investors, and policymakers to establish and advance global standards for corporate accountability.

The RDR Corporate Accountability Index offers a roadmap for companies to build and operate internet platforms and services that respect and protect human rights. The 2019 RDR Index ranked 24 companies on 35 indicators,¹ using a rigorous, seven-step [research process](#) and an [open methodology](#) that looked at companies' governance mechanisms to identify and prevent potential threats to users' human rights, plus disclosed policies affecting users' freedom of expression and privacy.

1.1 About this pilot study

This report presents research conducted on draft indicators aimed at setting corporate transparency and accountability standards for targeted advertising and algorithmic systems.² These draft indicators were published in October 2019, as part of our ongoing work to expand the RDR Index methodology to include new issues and new company types.³

On terminology:

In this report, we use the term “**algorithmic systems**” to mean the broader systems that use algorithms, machine learning, and/or related technologies to automate, optimize, and/or personalize decision-making processes. This includes automated decision-making technologies, which make decisions without significant human oversight or input, such as through the use of artificial intelligence.

See Section 8 of this report for an additional list of key terms.

¹ 2019 RDR Index, May 2019, <https://rankingdigitalrights.org/index2019/>.

² “Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems,” *Ranking Digital Rights*, October 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-_Targeted-advertising-algorithms.pdf.

³ Details of our methodology development work can be found on our website: <https://rankingdigitalrights.org/methodology-development/2020-revisions/>

In early 2019, we began a process of expanding the RDR Index methodology to include benchmarks that hold companies accountable for their targeted advertising policies and practices, and for their use and development of algorithmic systems. Our goal is to set global accountability and transparency standards, grounded in international human rights frameworks,⁴ for how major, publicly traded digital platforms and telecommunications companies can demonstrate respect for human rights online as they develop and deploy these new technologies.

1.2 Why we are adding new indicators on targeted advertising and algorithmic systems

Companies that derive revenue from targeted advertising collect and process vast amounts of personal data so that they can manage, shape, and govern the flow of content and information on their platforms in a way that maximizes ad revenue.⁵ They are able to do so with the assistance of algorithmic systems—and the use of these systems has enormous potential to harm users' fundamental human rights to free expression, information, and privacy, as well as to non-discrimination.⁶

Indeed, many of today's most vexing policy issues—including hate speech, disinformation, and other forms of media manipulation—stem from a business model that is based on the (often non-consensual) collection and use of personal information at scale.⁷ This mass corporate surveillance allows advertisers and other third parties to micro-target individuals with messages tailored to their specific attributes, traits, and preferences. These systems can amplify, prioritize, and otherwise shape content according to data- and machine-driven inferences about a user's preferences or personal traits. Platforms that optimize content based on popularity can be vulnerable to disinformation campaigns, hate speech, and other problematic content, which can unfairly influence public opinion, undermine democratic processes, and cause a range of human rights harms.

For this reason, RDR is expanding the RDR Index methodology to include developing new indicators that set global accountability and transparency standards for how tech companies can demonstrate respect for human rights as they develop and deploy these new technologies.

We intend to integrate new indicators into the revised 2020 RDR Index, set for release in February 2021. RDR's work in this area also informs the efforts of other stakeholders: investors conducting due diligence on portfolio risk, policymakers seeking to establish regulatory frameworks to protect the individual and collective rights of internet users, and

⁴ Universal Declaration of Human Rights, <https://www.un.org/en/universal-declaration-human-rights/>; International Covenant on Civil and Political Rights, <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

⁵ [Human Rights Risk Scenarios: Targeted Advertising](#), *Ranking Digital Rights* (2019).

⁶ [Human rights risk scenarios: Algorithms, machine learning and automated decision-making](#), *Ranking Digital Rights* (2019).

⁷ Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY, USA: PublicAffairs.

activists looking to encourage companies to pursue alternative business models and to mitigate the human rights harms associated with targeted advertising.

1.3 Stakeholder engagement process

The draft indicators on targeted advertising and algorithmic systems are the result of extensive consultations with a broad range of civil society, academic, industry, and policy experts conducted since early 2019. This process began with the release of consultation documents for targeted advertising and algorithmic systems.⁸ These documents outlined key human rights risk scenarios and proposed best practices to mitigate the identified risks.⁹ These best practices helped form the basis of the draft indicators that were used to evaluate companies for this pilot study.

1.4 Next steps

After extensive review and stakeholder consultation, the draft indicators were tested in a pilot study, the results of which are described in this report. Results of this pilot will be further analyzed by the RDR research team, taking into account feedback we receive from stakeholders. In April 2020, we will publish a full draft of the 2020 RDR Index methodology, followed by a period of public consultation. We plan to finalize the 2020 RDR Index methodology in May 2020. We welcome input or feedback about research presented in this study or the methodology at methodology@rankingdigitalrights.org.

⁸ All consultation documents can be accessed on the RDR website: <https://rankingdigitalrights.org/methodology-development/2020-revisions/>

⁹ [Human Rights Risk Scenarios: Targeted Advertising](#) and [Human rights risk scenarios: Algorithms, machine learning and automated decision-making](#), *Ranking Digital Rights* (2019).

2. Pilot study: Background and overview

2.1 Goals

The primary goal of this pilot was to test the set of draft indicators on targeted advertising and algorithmic systems in order to assess company disclosure of relevant policies and to determine additional methodology revisions required. Piloting these draft indicators enabled us to further evaluate standards for corporate accountability and transparency on these issues, as well as to assess the feasibility of incorporating new indicators into the 2020 RDR Index methodology.

2.2 Company selection

Five U.S. digital platforms and three European telecommunications companies were chosen for the pilot. For each company, we evaluated global group-level policies for the relevant indicators, as well as the home-country policies for selected services.

Platforms:

- Apple (iOS)
- Google (Search, YouTube, Android)
- Facebook (Facebook)
- Microsoft (Bing, OneDrive)
- Twitter (Twitter)

Telecommunications companies:

- Deutsche Telekom Germany (postpaid mobile)
- Telefónica Spain (postpaid mobile)
- Vodafone UK (postpaid mobile)

In selecting the above companies and services, we considered the following:

- *Company and service type:* Given the nature of the issues addressed in these draft indicators, we chose to pilot the major U.S. platforms ranked in the RDR Index. We selected specific services offered by these companies in order to test the applicability of different service types to these draft indicators.
- *Level of disclosure:* Companies were also selected for their level of disclosure on key issues addressed in these draft indicators. The 2019 RDR Index included two elements in one indicator (G4) that addressed human rights due diligence by companies on their targeted advertising policies and on their development and use of algorithms.¹⁰ Because our research showed that European telecommunications companies were among the few to conduct risk assessments of their use of algorithms, we opted to include three European telecommunications companies in this pilot study.

¹⁰ See Indicator G4, 2019 RDR Index, <https://rankingdigitalrights.org/index2019/indicators/g4/>.

2.3 Research steps

Research for this pilot was based on our evaluation of companies' own publicly available policies and disclosed commitments. Following our process for RDR Index research,¹¹ research for this pilot was conducted with a multi-step process of data collection, cross-checking, company feedback, and quality control:

- **Step 1: Data collection.** Primary researchers collected data on publicly available policies for each company and provided a preliminary evaluation of company disclosure across all indicators.
- **Step 2: Secondary review.** Secondary researchers conducted a fact-check of Step 1 evaluations.
- **Step 3: Reconciliation/horizontal review.** Differences between assessments conducted in Steps 1 and 2 were addressed and resolved. Indicators were then cross-checked to ensure they were evaluated consistently for each company.
- **Step 4: Company feedback.** All of the companies included in the pilot were offered the opportunity to provide written and verbal feedback about our evaluation. Preliminary evaluations were sent to companies for comment and feedback.
- **Step 5: Second horizontal review.** Indicators were cross-checked a second time to ensure they were evaluated consistently for each company.
- **Step 6: Final evaluations.** Final decisions were made about each company's evaluation.

2.4 Company evaluation and results

For the purposes of this pilot study, RDR chose companies and services to evaluate across select draft indicators depending on the nature of the indicator and on what questions or issues we wished to test. For these reasons, not every company and service was evaluated for every draft indicator. In the results presented in this report, we indicate which companies and services were piloted for different indicators and elements evaluated.

In addition, the draft indicators published in October 2019 included a wider set of revised indicators not pertaining directly to targeted advertising and algorithmic systems. Only the indicators that specifically focus on company policies and practices pertaining to targeted advertising and their use of algorithmic systems are presented in this pilot report.¹²

¹¹ See 2019 Research Process, Ranking Digital Rights, <https://rankingdigitalrights.org/2019-research-process/>.

¹² "Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems," *Ranking Digital Rights*, October 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-_Targeted-advertising-algorithms.pdf.

Finally, because this research is based on draft indicators that have not been formally incorporated into our methodology, we did not assign companies scores on their evaluation. For this reason, no company scores are presented in this study. Rather, findings are qualitative as RDR continues to assess how to integrate new indicators into the RDR Index methodology.

3. Summary of findings

This pilot study presents research on five U.S. platform companies (**Apple, Facebook, Google, Microsoft, and Twitter**) and three European telecommunications companies (**Deutsche Telekom, Telefónica, and Vodafone**). Companies were evaluated across three categories—governance, freedom of expression and information, and privacy—on a total of 25 draft indicators that set transparency and accountability standards for how companies develop and deploy algorithmic systems and their targeted advertising policies and practices.¹³ Findings are based on our evaluation of companies' own publicly available policies and disclosed commitments.

Overall, pilot results show that:

1. Companies lack strong governance and oversight mechanisms to ensure their business models and use of algorithmic systems do not contribute to or exacerbate human rights harms. Compared to European companies, U.S. platforms lack strong governance and oversight over how new technologies and targeted advertising-based business models affect fundamental human rights. Specifically, we note:

- **Governance gaps:** None of the five U.S.-based platforms evaluated make explicit public commitments to protect human rights as they develop and use algorithmic systems. European telecommunications companies **Telefónica** and **Vodafone**, however, do make clear commitments to respect and protect human rights as they develop and deploy these technologies—which puts these companies ahead of U.S. platforms in this area.
- **Weak human rights due diligence:** Companies operating major global platforms do not provide evidence that they are conducting risk assessments that enable them to understand and mitigate human rights harms associated with how their use of algorithmic systems and targeted advertising-based business models affect internet users around the world. Only one U.S. company (**Microsoft**) disclosed that it conducts impact assessments on its development and use of algorithmic systems. None of the eight companies in this pilot disclosed whether they conduct risk assessments on how their targeted advertising policies and practices affect users' freedom of expression and information rights, or their right to privacy, or to non-discrimination.

2. Companies lack transparency and accountability about how their targeted advertising policies and practices and their use of algorithmic systems shape online content. Unaccountable and unconstrained targeted advertising business models can result in the amplification of sensationalistic and inflammatory content in order to optimize user engagement and maximize profits. This can result in the dissemination of problematic, even illegal content that can unfairly influence public opinion, undermine democratic processes, and violate internet users' human rights. These harms can result from poor transparency and unclear rules and enforcement practices with regard to who

¹³ "Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems," *Ranking Digital Rights*, October 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-_Targeted-advertising-algorithms.pdf.

is allowed to advertise with what content on a platform. Unclear targeted advertising rules and enforcement may maximize revenue, but can also lead to the dissemination of content that creates additional human rights harms—including the spread of speech that discriminates against specific groups or communities, incites violence, or is intended to intimidate or mislead in ways that discourage or prevent people from exercising their human rights. Specifically, we note:

- **Opaque enforcement of ad-targeting rules:** Most companies disclosed some information about their ad-targeting rules but far less about what actions they take to enforce them. No company disclosed any data about what actions they take to remove ad content that violates targeting rules, which makes it impossible to hold companies accountable for enforcing their own ad-targeting policies and for rights violations that occur as a result of non-enforcement.
- **Lack of clarity about how algorithmic systems are deployed:** Companies did not disclose clear policies describing how algorithms are used across their platforms and services. While most platforms disclosed that they use algorithmic systems to rank or prioritize content, they did not provide users with clear explanations of how these systems work or with clear options for users to control whether and how content is curated.

3. Companies lack transparency and accountability about how they develop, share, and deploy user profiles. Digital platforms and telecommunications companies collect troves of data about users—from their location information to what websites they visit. Companies process this information into sophisticated profiles on individuals, with the help of algorithmic systems that make data-driven inferences, or predictions, about an individual's preferences, opinions, or traits. Advertisers, political strategists, and other third parties can use these profiles to target individuals or groups with tailored messages and content. These processes can not only pose significant risks to privacy—particularly when companies collect data and make inferences without users' knowledge or consent—but can also result in discriminatory outcomes if algorithmic systems are based on biased data sets. Specifically, we note:

- **Lack of disclosure about how algorithms are developed:** No company disclosed a clear policy with guidelines for how they develop and train their algorithmic systems—and most companies disclosed no options for users to control how their information is used for the development of these systems.
- **Lack of user control over inferred data:** Although slightly more than half of the piloted companies disclosed at least some information regarding what types of user information they use to make inferences and how they do so, just one (**Telefónica**) gave users any option to control whether their information can be subject to inference in the first place.
- **Unclear options to control ad targeting:** No company clearly disclosed whether targeted advertising is on or off by default, nor did any company disclose whether it allows users to opt in to being shown targeted advertising content.

4. Companies lack strong commitments to digital literacy. Companies take no extra steps to ensure users are fully informed about how companies' targeted advertising policies and their use of algorithmic systems affect users' freedom of expression, information, and privacy rights. Specifically, we note:

- No company published any materials that help educate users of freedom of expression-related risks associated with targeted advertising or algorithmic systems. Just two of eight companies (**Apple** and **Facebook**) published materials to help educate users on how to protect themselves from the privacy risks associated with targeted advertising. But no company provided materials to educate users about privacy risks associated with algorithmic system development.

The results of our research are presented in detail below.

4. Governance

The Governance category of the RDR Index evaluates whether companies have strong governance and oversight over freedom of expression and information and privacy issues across the company's global operations. It includes six indicators evaluating disclosure of commitments to freedom of expression and privacy principles, along with measures taken to implement those commitments.¹⁴

As part of RDR's ongoing methodology development work, we revised and expanded the indicators in this category to include benchmarks for corporate governance and oversight over how targeted advertising and development and deployment of algorithms affect fundamental freedom of expression and privacy rights. Specifically, we added one new element to existing Indicator G1,¹⁵ and developed a group of new human rights risk assessment indicators, building off the existing Indicator G4 and addressing due diligence best practices for companies' use of targeted advertising and algorithmic systems.¹⁶

Results of our pilot research on new indicators and elements in this category are further detailed below.

4.1 Policy commitment: Algorithmic systems and human rights

Companies are increasingly adopting policies outlining broad commitments to “ethical” or “responsible” use of artificial intelligence and other types of automation. However, there is a growing consensus among advocates and experts that international human rights standards and norms offer a more universally applicable and accountable framework for the development and use of these technologies.¹⁷ The Council of Europe, for instance, recommends that companies adopt human rights-centered principles and frameworks to guide the development and use of algorithmic systems.¹⁸

Existing Indicator G1 of the RDR Index expects companies to disclose a formal policy commitment to protect and respect users' fundamental rights to freedom of expression and privacy, in line with standards outlined in the UN Guiding Principles for Business and Human Rights.¹⁹ RDR has expanded this indicator to include similar standards for companies' development and use of algorithmic systems. Draft Element 3 (see *box below*) looks for companies to publish a clear commitment to respect and protect

¹⁴ The RDR Index, Governance: <https://rankingdigitalrights.org/index2019/categories/governance/>.

¹⁵ <https://rankingdigitalrights.org/2019-indicators/#G1>.

¹⁶ <https://rankingdigitalrights.org/2019-indicators/#G4>.

¹⁷ See, for example: “Human Rights in the Age of Artificial Intelligence,” *Access Now* (2018) <https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf>; Rebecca MacKinnon, “Ethics’ and ‘AI’: Can We Use These Terms to Take Effective Action?,” *Los Angeles Review of Books*, <https://blog.lareviewofbooks.org/provocations/ethics-ai-can-use-terms-take-effective-action/>.

¹⁸ “Addressing the impacts of Algorithms on Human Rights: Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems,” Council of Europe, Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence (2019), <https://rm.coe.int/draft-recommendation-of-the-committee-of-ministers-to-states-on-the-hu/168095eecf>.

¹⁹ “Guiding Principles on Business and Human Rights: Implementing the United Nations ‘Protect, Respect and Remedy’ Framework,” *United Nations* (2011), https://www.ohchr.org/documents/publications/guidingprinciplesbusinessshr_en.pdf.

international human rights standards and norms as they develop and deploy these technologies.

G1, Element 3: Does the company publish a clear commitment to human rights governing the use and development of algorithmic decision-making systems?²⁰

Key findings

Most companies fall short of formally committing to protect human rights as they develop and deploy algorithmic systems. In this area, European telecommunications companies are ahead of U.S. platform companies, which lacked clear commitments to human-rights centered policies to guide their development and use of algorithmic systems.²¹

Among the five U.S. platform companies evaluated, only two—**Google** and **Microsoft**—published overarching “AI principles” policies, which outline their broader approach to developing and using these technologies. However, these policies fell short of stating that human rights are the grounding principle guiding the development and use of these systems. In its “AI principles” policy, Google disclosed a commitment not to develop systems that are likely “to cause overall harm,” which includes developing “technologies whose purpose contravenes widely accepted principles of international law and human rights.”²² However, it is not clear whether human rights standards are the guiding framework that governs Google’s development and use of algorithmic systems.

Likewise, **Microsoft’s** “AI principles” policy states that it “takes into account” human rights when developing and using artificial intelligence.²³ However, like with Google, this policy falls short of committing to protect human rights as the guiding framework for Microsoft’s development and use of these technologies.

For the other three U.S. platform companies evaluated—**Apple**, **Facebook**, and **Twitter**—RDR was not able to locate a formal human rights commitment governing their AI development and use. This is especially notable for Facebook, given its extensive use of algorithms for its advertising services and News Feed. Facebook disclosed some information about how it uses algorithmic systems to curate content that appears on users’ News Feed (*see more in Section 5.4*) but did not disclose an overarching policy

²⁰ To see Elements 1 and 2 of Indicator G1: <https://rankingdigitalrights.org/2019-indicators/#G1>.

²¹ The following companies were evaluated for this element: Apple, Deutsche Telekom, Facebook, Google, Microsoft, Telefónica, Twitter, and Vodafone.

²² “Artificial Intelligence at Google: Our principles,” Google, <https://ai.google/principles/>, last accessed on March 3, 2020.

²³ “AI principles,” Microsoft, <https://www.microsoft.com/en-us/ai/our-approach-to-ai>, last accessed March 3, 2020.

commitment to protect users' freedom of expression, information, or privacy rights as it develops and deploys these technologies.

Likewise, in its "Defining public interest on Twitter" policy, **Twitter** disclosed that in some cases it allows Tweets that violate its terms to remain on Twitter because they are in the public interest, and in these cases, it will "take steps to make sure the Tweet is not algorithmically elevated on our service, to strike the right balance between enabling free expression, fostering accountability, and reducing the potential harm caused by these Tweets."²⁴ But this does not constitute a policy commitment addressing the company's human rights commitment that we look for in this element.

By comparison, **Telefónica's** "AI Principles" policy disclosed a clear commitment to respect human rights, stating: "We are strongly committed to respecting Human Rights, as is stated in our Business Principles and our Human Rights Policy, as well as all other internal policies that have been derived therefrom."²⁵

Similarly, in June 2019 **Vodafone** published its "Artificial Intelligence Framework," which lists the protection of human rights as one of its main pillars.²⁶ According to the policy: "By introducing this framework we are seeking to ensure that the AI technologies Vodafone creates and uses now and in the future fully respect the human rights of our customers, particularly their privacy and security, but also protects them from any unintended consequences from utilising machine learning techniques."²⁷

Deutsche Telekom Germany disclosed a framework for responsible AI development and use,²⁸ but like the U.S. platforms we evaluated, the company did not mention the protection of human rights as a guiding principle in this policy. In addition, the company published a blog post describing its own approach to "Digital Ethics" in its development and use of AI across the company's operations, but this also did not highlight human rights commitments.²⁹

4.2 Human rights due diligence

Indicator G4 in the RDR Index evaluates whether companies conduct human rights due diligence in order to identify and mitigate human rights harms posed by their business, products, or services.³⁰ The expanded draft Indicator G4 evaluates companies' due diligence practices pertaining to government regulations (G4a); of their own policy

²⁴ "Defining public interest on Twitter," Twitter, https://blog.twitter.com/en_us/topics/company/2019/publicinterest.html, last accessed March 3, 2020.

²⁵ "AI Principles," Telefónica, <https://www.telefonica.com/en/web/responsible-business/our-commitments/ai-principles>.

²⁶ "Vodafone launches Artificial Intelligence framework," Vodafone, June 11, 2019, <https://www.vodafone.com/perspectives/blog/vodafone-launches-artificial-intelligence-framework>.

²⁷ "Artificial Intelligence Framework," Vodafone, https://www.vodafone.com/content/dam/vodcom/images/public-policy/artificial-intelligence-framework/55678_Vodafone_AI_Framework_AW1_V3.pdf

²⁸ "Guidelines for Artificial Intelligence," Deutsche Telekom, <https://www.telekom.com/en/company/digital-responsibility/details/artificial-intelligence-ai-guideline-524366>.

²⁹ "Digital Ethics': Deutsche Telekom defines its own policy for the use of artificial intelligence," Deutsche Telekom, November 5 2018: <https://www.telekom.com/en/company/digital-responsibility/details/we-need-a-digital-ethics-policy-524364>

³⁰ Indicator G4: <https://rankingdigitalrights.org/2019-indicators/#G4>.

enforcement (G4b); of their targeted advertising policies and practices (G4c); and of their algorithmic systems.³¹

The box below displays the text of draft indicators G4c and G4d, which evaluate company due diligence on targeted advertising policies and practices (G4c) and on their development and use of algorithms (G4d), respectively. It is followed by key findings of our pilot research on those indicators.

Draft G4 indicators: Human rights due diligence

- **G4(c). Impact assessment: Targeted advertising:** The company should conduct regular, comprehensive, and credible due diligence, such as through robust human rights impact assessments, to identify how all aspects of its targeted advertising policies and practices affect users' fundamental rights to freedom of expression and information, to privacy, and to non-discrimination, and to mitigate any risks posed by those impacts.
- **G4(d). Impact assessment: Algorithmic decision-making systems:** The company should conduct regular, comprehensive, and credible due diligence, such as through robust human rights impact assessments, to identify how all aspects of its policies and practices related to the development and use of algorithmic decision-making systems affect users' fundamental rights to freedom of expression and information, to privacy, and to non-discrimination, and to mitigate any risks posed by those impacts.

To see the full draft methodology, including the list of elements and a glossary of terms for each indicator: "Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems," Ranking Digital Rights, October 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-_Targeted-advertising-algorithms.pdf.

Key findings

Most companies are not well positioned to understand and mitigate human rights harms associated with how their use of algorithmic systems and advertising-based business models affect internet users around the world.³²

No company evaluated in this pilot met baseline standards of transparency regarding their human rights due diligence policies and practices across all of the issues addressed in

³¹ See full draft methodology: "Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems," Ranking Digital Rights, October 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-_Targeted-advertising-algorithms.pdf.

³² Companies piloted on these indicators: Apple, Deutsche Telekom, Facebook, Google, Microsoft, Telefónica, Twitter, and Vodafone.

this group of indicators. Only three of the eight companies evaluated—**Deutsche Telekom**, **Microsoft**, and **Telefónica**—disclosed some information about assessing human rights risks associated with their development and use of algorithmic systems (G4d). Not a single company disclosed if they assess human rights risks associated with their targeted advertising policies and practices (G4c).

Telefónica stood out for its comparatively strong disclosure of its risk assessment procedures related to its development and use of these technologies. The company clearly disclosed that it assesses the freedom of expression, privacy, and discrimination risks associated with these systems, and that it conducts additional evaluations whenever these assessments identify concerns.³³

Microsoft also disclosed that it began to conduct human rights risk assessments on its development and use of artificial intelligence in 2017.³⁴ According to the company’s annual Human Rights Report, the goals of these assessments were to identify the human rights risks of developing and deploying automation, and to “position the responsible use of AI as a technology in the service of human rights.”³⁵

Deutsche Telekom disclosed that it assesses privacy risks related to its AI systems, but did not reveal evidence of assessing the impacts of these systems on users’ fundamental rights to freedom of expression, information, and non-discrimination.³⁶ The company’s “Guidelines for Artificial Intelligence” policy states that the “essential paradigm for our AI systems’ impact analysis is ‘privacy and security by design,’” and that the company “takes great care in the initial algorithm of our own AI solutions to prevent so called ‘Black Boxes’ and to make sure that our systems shall not unintentionally harm the users.”³⁷

The lack of human rights due diligence by other U.S. platforms is notable. Previous RDR Index research has shown that while **Google** and **Facebook** conduct risk assessments on some aspects of the regulatory environments of the markets in which they operate, neither company disclosed evidence of conducting risk assessments of their own policies—which includes their targeted advertising policies and practices or their use and development of algorithmic systems.³⁸

The RDR Index has highlighted **Twitter**’s especially poor disclosure, particularly in relation to other U.S. platforms, about whether and how it conducts any due diligence on the company’s human rights impacts and risks.³⁹ As noted In the 2019 RDR Index, Twitter

³³ Integrated Management Report, Telefónica (2018)

<https://www.telefonica.com/documents/153952/13347920/Telefonica-Integrated-Management-Report-2018.pdf>.

³⁴ “Global Human Rights Statement,” Microsoft,

<https://www.microsoft.com/en-us/corporate-responsibility/human-rights-statement>.

³⁵ “Global Human Rights Statement,” Microsoft,

<https://www.microsoft.com/en-us/corporate-responsibility/human-rights-statement>.

³⁶ “Guidelines for Artificial Intelligence,” Deutsche Telekom,

<https://www.telekom.com/en/company/digital-responsibility/details/artificial-intelligence-ai-guideline-524366>.

³⁷ “Guidelines for Artificial Intelligence,” Deutsche Telekom,

<https://www.telekom.com/en/company/digital-responsibility/details/artificial-intelligence-ai-guideline-524366>.

³⁸ See “Due Diligence” section of the 2019 RDR Index report:

<https://rankingdigitalrights.org/index2019/report/governance/#section-33>.

³⁹ See Twitter’s G4 scores in the 2019 RDR Index: <https://rankingdigitalrights.org/index2019/indicators/g4/>

disclosed the least information about its due diligence efforts of any U.S. company evaluated.⁴⁰ The company did not reveal anything about whether it conducts assessments of risks associated with its targeted advertising practices and policies (G4c) or about its development and use of algorithmic systems (G4d).

⁴⁰ See “Due Diligence” section of the 2019 RDR Index report:
<https://rankingdigitalrights.org/index2019/report/governance/#section-33>.

5. Freedom of expression and information

The Freedom of Expression and Information category of the RDR Index evaluates whether companies demonstrate concrete ways in which they respect users' right to freedom of expression and information, as articulated in the Universal Declaration of Human Rights,⁴¹ the International Covenant on Civil and Political Rights,⁴² and other international human rights instruments.⁴³ A company's disclosed policies should demonstrate how it works to avoid contributing to actions that may interfere with this right, except where such actions are lawful, proportionate, and for a justifiable purpose. Companies that perform well in this category demonstrate a strong public commitment to transparency, not only in terms of how they comply with laws and regulations or respond to government demands, but also how they determine, communicate, and enforce private rules and commercial practices that affect users' freedom of expression.

The draft indicators published in October 2019 introduced a number of revisions to this category to include transparency and accountability standards for companies' targeted advertising policies and practices and for their development and use of algorithmic systems.⁴⁴ In addition to our existing indicators that ask companies to clearly disclose terms of service policies governing users' speech and activities and how those rules are enforced, we developed new indicators that ask companies to disclose their policies for what advertising content is permitted, policies for how users can or cannot be targeted for advertising (advertising targeting policies), and policies for how algorithmic systems are used (algorithmic system use policies).

We also drafted three new indicators evaluating company transparency about algorithmic content curation, recommendation, and ranking systems (F12); company policies governing the use of automated software agents ("bots") on their platforms and the enforcement of such policies (F13); and company efforts to advance media literacy by educating users on how to protect themselves from advertisers' attempts to mislead them and from risks associated with the use of algorithms, machine learning and automated decision-making (F14).

The box below, containing the text of the draft indicators in this category, is followed by a presentation of the results of pilot research on them.

⁴¹ Universal Declaration of Human Rights, <https://www.un.org/en/universal-declaration-human-rights/>

⁴² International Covenant on Civil and Political Rights, <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

⁴³ Freedom of expression category, RDR Index, <https://rankingdigitalrights.org/index2019/categories/freedom-of-expression/>

⁴⁴ "Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems," Ranking Digital Rights, October 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-_Targeted-advertising-algorithms.pdf.

Freedom of expression and information category—Draft indicators on targeted advertising and algorithmic systems

- F1b. Access to advertising content policies
- F1c. Access to ad targeting policies
- F1d. Access to algorithmic system use policies
- F2b. Changes to ad content policies
- F2c. Changes to ad targeting policies
- F2d. Changes to algorithmic system use policies
- F3b. Advertising content rules and enforcement
- F3c. Advertising targeting rules and enforcement
- F4c. Data about advertising content policy enforcement
- F4d. Data about advertising targeting policy enforcement
- F12. Algorithmic content curation, recommendation, and/or ranking systems
- F13. Automated software agents (“bots”)
- F14. Informing and educating users about risks

To see the full draft methodology: “Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems,” Ranking Digital Rights, October 2019, <https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators-Targeted-advertising-algorithms.pdf>.

Key findings

Companies lack transparency and accountability about how targeted advertising and algorithmic systems shape online content.

- **Companies lack disclosure of ad content and ad targeting policy enforcement.** While most platforms disclosed information about their ad content and ad targeting rules—including what types of audience categories advertisers and other third parties are not permitted to use for targeting ads—none disclosed data about their enforcement of these rules (see *Sections 5.1 and 5.2, below*).
- **Companies lack clear policies describing how algorithms are deployed across their products and services.** While some companies disclosed how

algorithms are used to perform certain functions—like curating or prioritizing content—no company disclosed an overarching policy describing how algorithms are used across the company’s products and services (see *Section 5.3 below*).

- **Companies do not give users clear options to control how algorithms shape content.** Most of the platforms evaluated disclosed that they use algorithms to rank and prioritize content on their services but lacked transparency about options for users to control the variables that influence how these systems rank and prioritize the content that they see (see *Section 5.4 below*).
- **Companies lack clear rules about platform manipulation.** Companies are not transparent about how they deal with bots on their platforms. While the platforms evaluated provided some information about guidelines governing the use of bots, this information was not comprehensive (see *Section 5.5 below*).
- **Companies make no efforts to advance digital literacy.** Companies disclosed no practical materials to help users better understand the human rights risks associated with targeted advertising and algorithmic systems (see *Section 5.6 below*).

5.1 Ad content policies and enforcement

Companies that enable any type of advertising on their services or platforms should clearly disclose the rules for what types of ad content is prohibited—for example, ads that discriminate against individuals or groups based on personal attributes like age, religion, gender, and ethnicity. Companies should be transparent about these rules so both users and advertisers can understand what types of ad content are not permissible and so they can be accountable for the ad content that appears on their services or platforms.

Therefore, companies should make their ad content policies easy to find and understand (F1b); should commit to notifying users when these rules change (F2b); should clearly disclose rules for what types of ad content are prohibited, as well as how they detect breaches to these rules (F3b); and should publish data on what actions they take to remove ad content when rules violations occur (F4c).

The full text of the draft indicators on advertising content policies is displayed below, followed by key findings of the pilot research on these indicators.

Draft indicators: Advertising content policies

- **F1(b). Access to advertising content policies:** The company should offer advertising content policies that are easy to find and easy to understand.
- **F2(b). Changes to advertising content policies:** The company should clearly disclose that it provides notice and documentation to users when it changes its advertising content policies.

- **F3(b). Advertising content rules and enforcement:** The company should clearly disclose its content policies governing third parties' use of advertising technologies on the platform.
- **F4(c). Data about advertising content policy enforcement:** The company should clearly disclose and regularly publish data about the volume and nature of actions taken to restrict advertising content that violates the company's advertising content policies.

To see the full draft methodology: "Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems," Ranking Digital Rights, October 2019, <https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators-Targeted-advertising-algorithms.pdf>.

Key findings

Companies lack accountability for the ad content that appears on their platforms and services. While most companies published rules about what types of ad content is prohibited, none published any data about actions they take to enforce these rules.

A review of publicly available policies for eight companies showed that most published ad content policies that were very easy to find (F1b)—but none disclosed any data about the volume and nature of the ad content removed for breaching these rules (F4c).⁴⁵

Among U.S. platforms—**Apple (iOS), Facebook, Google (Android, YouTube), and Twitter**—all disclosed *some* information about their advertising content policies, including what types of ad content is prohibited (F3b, Element 1), although companies disclosed less information about how they detect breaches to these rules (either through human or automated review) (F3b, Element 3). None published any data about actions they take to remove ad content or suspend advertiser accounts for rules violations (F4c).

U.S. platform companies were more transparent about their ad content rules than the three European telecommunications companies evaluated. Even though all three companies evaluated—**Deutsche Telekom Germany, Telefónica Spain, Vodafone UK**—offer mobile advertising services that enable advertisers to reach their customers via SMS-enabled messages, only one company (**Telefónica Spain**) disclosed ad content policies that included rules about what types of ad content is prohibited (F3b). None of these companies published any data about actions they take to remove ad content or suspend advertiser accounts for rules violations (F4c).

⁴⁵ The following U.S. platform companies/services were piloted for these indicators: Apple (iOS), Facebook (the social networking service); Google (YouTube), Google (Android); Twitter (Twitter). [Deutsche Telekom Germany](#), [Telefónica Spain](#), and [Vodafone UK](#) each offer mobile advertising services, which enable advertisers to reach their customers via SMS-enabled messages. For this reason, RDR opted to apply our draft indicators addressing advertising transparency to these companies' postpaid mobile services.

All companies also failed to disclose a commitment to notify users when their ad content policies change (F2b).⁴⁶ **Facebook’s** Advertising Policies “Things You Should Know” section states: “These policies are subject to change at any time without notice.”⁴⁷

5.2 Ad targeting policies and enforcement

In addition to looking at a company’s broader ad content policies, draft indicators also look for companies to disclose their specific ad targeting policies (see F1c, F2c, F3c, F4d below). The ability for advertisers or other third parties to target users with tailored content—based on their browsing behaviors, location information, and other data and characteristics that have been inferred about them⁴⁸—can significantly shape a user’s online ecosystem. Targeting, which can include both paid and unpaid content, can amplify offline social inequities and can be overtly discriminatory. It can also result in so-called “filter bubbles” as well as amplify problematic content, including content intended to mislead or to spread falsehoods.⁴⁹

Therefore, companies that enable advertisers and other third parties to target users with tailored ads or content should publish targeting policies that users can easily find and understand (F1c), and commit to notify users of changes to these policies (F2c). Policies should clearly disclose what types of ad targeting is not permitted—including listing restrictions against using certain audience categories—and how a company identifies breaches to these rules (F3c). Companies should also publish data about what actions it takes to remove ad content or to disable accounts when its ad targeting rules are breached (F4d) so that they can be held accountable for enforcing these policies.

The full text of the draft indicators on ad targeting transparency and accountability is displayed below, followed by findings of the pilot research on them.

Draft indicators: Ad targeting transparency and accountability

F1(c). Access to advertising targeting policies: The company should offer advertising targeting policies that are easy to find and easy to understand.

F2(c). Changes to advertising targeting policies: The company should clearly disclose that it provides notice and documentation to users when it changes its advertising targeting policies.

⁴⁶ “Google Ads policy,” Google, <https://support.google.com/adspolicy/answer/6008942?hl=en>, last accessed March 3, 2020.

⁴⁷ “Advertising Policies,” Facebook, https://www.facebook.com/policies/ads/prohibited_content, last accessed March 3, 2020.

⁴⁸ For more about data inference policies, Section 6.2 of this report.

⁴⁹ “Draft Indicators Transparency and accountability standards for targeted advertising and algorithmic decision-making systems,” Ranking Digital Rights, https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-_Targeted-advertising-algorithms.pdf, last accessed March 11, 2020.

F3(c). Advertising targeting rules and enforcement: The company should clearly disclose its targeting policies governing third parties' use of advertising technologies on its products and services.

F4(d). Data about advertising targeting policy enforcement: The company should clearly disclose and regularly publish data about the volume and nature of actions taken to restrict advertising content that violates the company's advertising targeting policies.

To see the full draft methodology, including the list of elements for each indicator and a glossary of terms, see: "Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems," *Ranking Digital Rights*, October 2019, <https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators-Targeted-advertising-algorithms.pdf>.

Key findings

Companies lack transparency about if and how they enforce their ad targeting rules. U.S. platforms disclosed more than European telecommunications companies about ad targeting rules, but most companies evaluated in the pilot lacked transparency about how breaches to those rules are detected. No company disclosed any data about what enforcement actions they take when rules violations occur.⁵⁰

All of the four U.S. platforms evaluated on these indicators—**Apple (iOS), Facebook, Google (YouTube, Android), and Twitter**—disclosed the fact that users will be targeted with interest-based or tailored content (F3c, Element 1). Each of these platforms also gave some information about what targeting parameters are not permitted (F3c, Element 2). But they disclosed less about how they detect breaches to these rules (F3c, Element 6) and published no enforcement evidence: no company provided any data about the volume and nature of ad content removed or advertiser accounts suspended once violations are discovered (F4d).

The full text of all elements for draft indicator F3c is displayed below.

Draft Indicator F3(c): Advertising targeting rules and enforcement

The company should **clearly disclose** its targeting policies governing **third parties'** use of **advertising technologies** on its products and services.

⁵⁰ For these indicators, we piloted the following: Apple (iOS); Facebook (the social networking service); Google (YouTube, Android); Twitter (the social networking service). [Deutsche Telekom Germany](#), [Telefónica Spain](#), and [Vodafone UK](#) each offer mobile advertising services, which enable advertisers to reach their customers via SMS-enabled messages. For this reason, RDR opted to apply our draft indicators addressing advertising transparency to these companies' postpaid mobile services.

Elements:

1. Does the company **clearly disclose** whether users will be shown **advertising content** based on their browsing history, location information, social media use, demographic characteristics, or other **user information**?
2. Does the company **clearly disclose** what types of **targeting parameters** are not permitted?
3. Does the company **clearly disclose** that it does not permit advertisers to target specific individuals?
4. Does the company **clearly disclose** that algorithmically generated **advertising audience categories** are evaluated by human reviewers before they can be used?
5. Does the company **clearly disclose** its guidelines for evaluating algorithmically generated **advertising audience categories** to ensure they do not contribute to human rights harms?
6. Does the company **clearly disclose** information about the processes and technologies it uses to identify **advertising content** or accounts that violate the company's rules?

To see the full draft methodology, including a glossary of the above key terms highlighted in **bold**, see: "Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems," *Ranking Digital Rights*, October 2019, <https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators-Targeted-advertising-algorithms.pdf>.

Our pilot research on these elements found the following::

- **Apple** disclosed that iOS users will be shown targeted ads (F3c, Element 1) and listed information that advertisers are prohibited from using in their targeting—including users' sexual orientation, religious beliefs, or political affiliations (F3c, Element 2).⁵¹
- **Google** disclosed that YouTube and Android users will be targeted with interest-based or "personalized ads" (F3c, Element 1), and that "advertisers can't use sensitive interest categories to target ads to users or to promote advertisers' products or services."⁵² ("Sensitive interest information" is defined as "personal hardships," "identity and belief," and "sexual interests.") (F3c, Element 2).
- **Twitter** disclosed that its users will be targeted with tailored ads, and provided rules about what types of audience categories advertisers are prohibited from using: "Our ads policies prohibit advertisers from targeting ads based on

⁵¹ "Advertising & Privacy," Apple, <https://support.apple.com/en-us/HT205223>

"App Store Review Guidelines," Apple, <https://developer.apple.com/app-store/review/guidelines>, last accessed March 3, 2020.

⁵² "Personalized Advertising," Google, <https://support.apple.com/en-us/HT205223>, last accessed March 3, 2020.

categories that we consider sensitive or are prohibited by law, such as race, religion, politics, sex life, or health.”⁵³ Its “Policies for keyword targeting” page provided additional information about prohibited audience categories.⁵⁴ However, Twitter’s ad policies and targeting rules are presented in numerous policies and webpages, which made understanding these rules challenging.⁵⁵

- **Facebook** was less transparent about its ad targeting rules than other platforms evaluated: it disclosed that users will be targeted with ads (F3c, Element 1) but less about the exact ad targeting parameters that are prohibited (F3c, Element 2). It disclosed that advertisers can tailor ads to “custom audiences” but are prohibited from using these targeting options “to discriminate against, harass, provoke, or disparage users or to engage in predatory advertising practices.”⁵⁶ However, the custom audience options were only visible when logged into the platform and therefore only available to Facebook account holders. Companies should make their policies—including their ad targeting rules—publicly available so users can access and evaluate those policies to make informed decisions about whether to join a particular platform or service.

Notably, none of these four platform companies explicitly prohibited advertisers from targeting specific individuals (F3c, Element 3). While **Google** disclosed it prohibits “hyper targeting”⁵⁷—or narrowing ad targeting to a small number of users—it also seems to offer advertisers the ability to target individual users through its “remarketing” feature (known by other companies as “retargeting”).

U.S. platforms also lacked clarity about how they detect breaches to ad targeting rules (F3c, Element 6). For instance, **Twitter** disclosed that users can report ads believed to violate the company’s policies but provided no additional information about other processes and technologies used to identify rules violations.⁵⁸ **Facebook** disclosed a detailed system for reviewing all ads for compliance with ad content policies, which includes ad targeting rules, before they are published. Its ad policy states: “we’ll check your ad’s images, text, targeting, and positioning, in addition to the content on your ad’s landing page.”⁵⁹ However, the company gave no further details describing what processes or technologies are used to review these ads, including if and how automation is used or if there is any human involvement.

⁵³“Privacy Policy,” Twitter, <https://twitter.com/en/privacy>, last accessed March 9, 2020.

⁵⁴ “Policies for keyword targeting,” Twitter, <https://business.twitter.com/en/help/ads-policies/other-policy-requirements/policies-for-keyword-targeting.htm>, last accessed March 3, 2020.

⁵⁵ Twitter’s ad targeting rules were found in its: [Privacy Policy](#), [Twitter Ads Policies](#), [Twitter Ads Approval](#), [About Twitter Ads offboarding](#), [Policies for keyword targeting](#), and [Policies for Conversion Tracking and Tailored Audiences](#), all last accessed March 3, 2020.

⁵⁶ “Ad Policies,” Facebook, <https://www.facebook.com/policies/ads/>, last accessed March 3, 2020.

⁵⁷ “Personalized advertising,” Google, https://support.google.com/adspolicy/answer/143465?hl=en&ref_topic=7012636, last accessed March 9, 2020.

⁵⁸ “Report Twitter Ads,” Twitter, <https://help.twitter.com/en/safety-and-security/reporting-twitter-ads>, last accessed March 9, 2020.

⁵⁹ “Ad Policies,” Facebook, <https://www.facebook.com/policies/ads/>, last accessed March 3, 2020.

None of the platforms evaluated published any data about actions they take to remove ad content or suspend advertiser accounts for breaching ad targeting rules (F4d).

Two of the three telecommunications companies evaluated—**Telefónica Spain** and **Vodafone UK**—disclosed that users will be shown advertising content but provided very little additional information beyond this. For instance, **Telefónica Spain** disclosed that users of its postpaid service will be targeted with ads—and it disclosed what types of user information it collects to build profiles on users for advertising purposes—but no further details could be found regarding its ad targeting rules (F3c, Elements 2 through Elements 6). The company did not publish any data about the enforcement of its ad targeting rules (F4d).

Vodafone UK disclosed that it may use “calling and messaging activities, location information and browsing information” to tailor their messages to users after obtaining their permission (F3c, Element 1),⁶⁰ but offered no more details about its ad targeting policies and practices (F3c, Elements 2 through 6). The company did not publish any data about the enforcement of its ad targeting rules (F4d).

RDR researchers were not able to locate any publicly available ad targeting policies for **Deutsche Telekom Germany’s** postpaid mobile service (F1c, F2c, F3c, F4d).

No company evaluated on these indicators disclosed if algorithmically generated advertising audience categories were evaluated by human reviewers (F3c, Element 4), or disclosed guidelines for evaluating algorithmically generated advertising audience categories to ensure they do not contribute to human rights harms (F3c, Element 5).

5.3 Algorithmic system use policies

Algorithmic systems can have adverse effects on fundamental human rights—and specifically, the rights to free expression and access to information as well as the right to non-discrimination.⁶¹ In addition to clearly committing to respect and protect human rights as they develop and deploy these technologies (see draft Indicator G1, Element 3), we expect companies to publish policies that clearly describe the terms for how they use algorithmic systems across their service and platforms. Similar to having terms of service policies or user agreements that outline the terms for what types of content or activities are not prohibited, companies that use algorithmic systems with the potential to cause human rights harms should publish a clear and accessible policy stating the nature and functions of these systems.⁶² This policy should be easy to find, presented in plain language, and contain options for users to manage settings.

⁶⁰ “Privacy Policy,” Vodafone UK, <https://www.vodafone.co.uk/privacy/#/privacy-policy>, last accessed March 3, 2020.

⁶¹ “Consultation draft: Human Rights Risk Scenarios: Algorithms, Machine Learning and Automated Decision-Making,” *Ranking Digital Rights* (2019), https://rankingdigitalrights.org/wp-content/uploads/2019/07/Human-Rights-Risk-Scenarios_-_algorithms-machine-learning-automated-decision-making.pdf.

⁶² “Addressing the impacts of Algorithms on Human Rights: Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems,” Council of Europe, Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence (2019), <https://rm.coe.int/draft-recommendation-of-the-committee-of-ministers-to-states-on-the-hu/168095eefc>.

Draft indicator F1d evaluates if companies have algorithmic system use policies that are easy to find and understand, and available in the main languages of the company's home market. Draft indicator F2d asks if companies commit to notify users when these policies change. The full text of both indicators is displayed below, followed by key findings of the pilot research on them.

Draft indicators addressing algorithmic system use policies

F1(d). Access to algorithmic system use policies: The company should offer policies related to their use of algorithms that are easy for users to find and understand.

F2(d). Changes to algorithmic system use policies: The company should clearly disclose that it provides notice and documentation to users when it changes its algorithmic system use policies.

To see the full draft methodology, including a glossary of the above key terms highlighted in **bold**, see: "Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems," *Ranking Digital Rights*, October 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-_Targeted-advertising-algorithms.pdf.

Key findings

While every company in this pilot deploys algorithms in various ways in its products and services, none disclosed a discrete policy or terms outlining guidelines for how they use these systems.⁶³ Some companies had limited disclosure of how they use algorithmic systems but none disclosed a discrete policy that clearly and prominently describes their terms of use for these systems.

Facebook, Google, Microsoft, and Twitter disclosed some information about how they use algorithms in certain functions on their services—such as in prioritizing content in a news feed or search engine (see draft Indicator F12 analysis below)—but none publish an overarching algorithmic “terms of use” policy describing terms for how algorithms are used across the company's products and services.

For a further discussion of our findings on these indicators, see **Section 7** which highlights the most challenging indicators and issues that arose during this pilot study.

⁶³ Companies/services piloted on these indicators: Apple (iOS), Google (Search, YouTube, Android), Facebook (Facebook), Microsoft (Bing, OneDrive), Twitter (Twitter), Deutsche Telekom Germany (postpaid mobile), Telefónica Spain (postpaid mobile), Vodafone UK (postpaid mobile).

5.4 Algorithmic content curation

Algorithmic curation, recommendation, and ranking systems play a critical role in shaping the digital content that users access and share. Studies show how systems that are optimized for user engagement can have the effect of amplifying and prioritizing controversial and inflammatory content, which can distort public discourse, amplify social divisions, and cause human rights harms.⁶⁴ Over time, algorithmic curation and recommendation systems that are optimized for engagement can significantly alter the news and information ecosystems for individuals, communities, or even entire countries. These systems can and have been manipulated to spread disinformation and to otherwise distort the information ecosystem, which can, in turn, undermine democracy and cause human rights harms and abuses.

Companies should therefore be transparent about and accountable for how algorithms shape the content that users are served, including about the variables that influence these systems. Draft indicator F12 asks companies to clearly disclose information about whether they use algorithmic content curation, recommendation, and ranking systems to shape content (Element 1); how they work, and what variables influence these systems (Element 2); and what options users have to control the variables these systems use to curate content (Element 3). Companies should also disclose whether such systems are on or off by default (Element 4), with “opt-in” being the preferred default option (Element 5). The full text of all elements of draft indicator F12 is displayed below, followed by key findings.

Draft indicator F12: Algorithmic content curation, recommendation, and/or ranking systems.

Companies should **clearly disclose** how online **content** is **curated, ranked, or recommended**.

Draft Elements:

1. Does the company disclose whether it uses **algorithmic** decision-making systems to **curate, recommend, and/or rank** the **content** that users can access through its platform?
2. Does the company **clearly disclose** how the **algorithmic content curation, recommendation, and/or ranking** system works, including the variables that influence it?
3. Does the company disclose what options users have to control the variables that the **algorithmic content curation, recommendation, and/or ranking** system takes into account?

⁶⁴ “Rising Through the Ranks - How Algorithms Rank and Curate Content in Search Results and on News Feeds,” Spandana Singh (October 2019), <https://www.newamerica.org/oti/reports/rising-through-ranks/>.

4. Does the company disclose whether automated content **curation, recommendation, and/or ranking** systems are *on* or *off* by default?
5. Does the company disclose that users can opt in to **automated content curation, recommendation, and/or ranking** systems?

To see the full draft methodology, including a glossary of the above key terms highlighted in **bold**, see: “Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems,” *Ranking Digital Rights*, October 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-_Targeted-advertising-algorithms.pdf.

Key findings

Platforms lack transparency and accountability about how algorithmic systems shape online information ecosystems. While most of the platforms evaluated disclosed that they use algorithms to rank and prioritize content on their services—although with varying degrees of clarity—most lacked transparency about options for users to control variables that influence how these systems rank and prioritize the content they are being delivered.⁶⁵

- **Facebook** disclosed that content that appears in the News Feed is algorithmically curated, (F12, Element 1), although it did not explicitly state that these systems are on by default (F12, Element 4).⁶⁶ However, Facebook did offer fairly detailed information about the factors that influence the News Feed's ranking system (F12, Element 2), and explained various ways for users to customize the content in their News Feed (F12, Element 3). For example, it disclosed how to set the News Feed to prioritize either content from people or from organizations.⁶⁷ It also stated that users cannot opt *in* to algorithmic content curation or ranking systems—which means this system is on by default (F12, Element 4 and Element 5).⁶⁸
- **Google** revealed more about the algorithmic curation systems for Search than for YouTube. For Search, the company disclosed that Search results are produced by using an algorithm-based ranking system (F12, Element 1),⁶⁹ and that this system is automatically *on* by default (F12, Element 4).⁷⁰ It listed several variables that influence Search results and gave additional resources for improving Search

⁶⁵ Companies/services piloted for this indicator (F12): Apple (iOS); Facebook (the social networking service); Google (Search, YouTube); Microsoft (Bing); and Twitter (the social networking service).

⁶⁶ “How News Feed Works,” Facebook, <https://www.facebook.com/help/964154640320617>, last accessed March 3, 2020.

⁶⁷ “Control What You See in News Feed,” Facebook, <https://www.facebook.com/help/964154640320617>, last accessed March 3, 2020.

⁶⁸ “Control What You See in News Feed,” Facebook, <https://www.facebook.com/help/964154640320617>, last accessed March 3, 2020.

⁶⁹ “How Search algorithms work,” Google, <https://www.google.com/search/howsearchworks/algorithms/>, last accessed March 3, 2020.

⁷⁰ “How Google Search works,” Google, <https://www.google.com/search/howsearchworks/>, last accessed March 3, 2020.

algorithms (F12, Element 2).⁷¹ However, it did not disclose options for users to control the variables that determine the Search rankings they obtain (F12, Element 3). RDR also could not locate any information about whether Google allows Search users to opt in to algorithmic curation (F12, Element 5).

For YouTube, Google did not specifically refer to the use of algorithms, AI, or automation (F12, Element 1), or disclose whether algorithmic curation systems are on or off by default (F12, Element 4). It also did not disclose what variables influence YouTube search results (F12, Element 2), but unlike for Search, it did disclose options for users to control these results (F12, Element 3).⁷² RDR could not locate any information about whether Google allows YouTube users to opt in to algorithmic curation (F12, Element 5).

- **Twitter** did not clearly disclose that algorithmic systems are used to curate Tweets on a user’s timeline (F12, Element 1).⁷³ It offered detailed information about the technology behind its algorithmic ranking in a post on its Engineering blog, but this policy is difficult for the average user to find or understand.⁷⁴ On the company’s more user-facing “About your Twitter Timeline” page, the company disclosed ways users can change how Tweets are viewed and adjust their timeline feed (F12, Element 3), but there was no mention that this curation is performed by an algorithmic system (F12, Element 1) or whether it is on or off by default (F12, Element 4).⁷⁵ However, Twitter did disclose options for users to choose whether to display algorithmically curated “top Tweets” or the latest Tweets (F12, Element 5).
- **Microsoft** disclosed some information about its search algorithms on a more technically oriented portal for its AI research⁷⁶ but did not say anything about its use of algorithms for content curation, recommendation, and/or ranking on Bing’s more user-facing policies, such as in the Microsoft Services Agreement (F12, Element 1 and Element 2).⁷⁷ Furthermore, Microsoft did not provide information on what options users have to control the search algorithm (F2, Element 3).
- For **Apple** (iOS), RDR could not locate any information about whether or how that platform uses algorithmic recommendation, curation, and/or ranking systems.

⁷¹ “Search Quality Evaluator Guidelines,” Google, <https://static.googleusercontent.com/media/guidelines.raterhub.com/en//searchqualityevaluatorguidelines.pdf>, last accessed March 3, 2020.

⁷² “Manage your recommendations and search results,” Google, <https://support.google.com/youtube/answer/6342839?co=GENIE.Platform%3DAndroid&hl=en>, last accessed March 3, 2020.

⁷³ “About your Twitter Timeline,” Twitter, <https://help.twitter.com/en/using-twitter/twitter-timeline>, last accessed March 3, 2020.

⁷⁴ “Using Deep Learning at Scale in Twitter’s Timelines,” Twitter, https://blog.twitter.com/engineering/en_us/topics/insights/2017/using-deep-learning-at-scale-in-twitters-timelines.html, last accessed March 3, 2020.

⁷⁵ “About your Twitter Timeline,” Twitter, <https://help.twitter.com/en/using-twitter/twitter-timeline>, last accessed March 3, 2020.

⁷⁶ “Application samples from AI Lab/Vector search,” Microsoft <https://www.microsoft.com/en-us/ai/ai-lab-application-samples?activetab=pivot1:primary7>, last accessed March 3, 2020.

⁷⁷ Microsoft Services Agreement, <https://www.microsoft.com/en-US/servicesagreement/>, last accessed March 3, 2020.

5.5 Bot policies

Draft indicator F13 asks companies to clearly disclose their policies for allowing bots on their platforms. While some bots are harmless, there are more problematic uses of bots, such as when political parties or their surrogates use botnets to promote certain messages or to artificially inflate a candidate’s reach in order to manipulate public discourse and outcomes.⁷⁸ On some social media platforms, bots or coordinated networks of bots (“botnets”) can be used to harass users (“brigading”), artificially amplify certain pieces of content (mass retweeting, etc.), and otherwise distort public discourse on the platform. Such distortions represent a violation of freedom of information, particularly when the result of those political outcomes includes empowerment of the winning group to violate the rights of other people. Some experts have called for companies to require users who use bots to explicitly label them as bots in order to help detect such distortions.

79

The full text of all elements used to evaluate indicator F13 is displayed below, followed by key findings.

Draft indicator F13: Bot policy

Companies should clearly disclose policies governing the use of automated software agents (“**bots**”) on their platforms, products and services, disclose how they enforce such policies, and engage in transparency reporting around the enforcement of such policies.

Elements:

1. Does the company **clearly disclose** a definition of a “bot”?
2. Does the company clearly disclose guidelines governing the use of **bots** to generate **content**, disseminate **content**, or perform other actions?
3. Does the company clearly disclose that it requires users to clearly label all **content** and **accounts** that are produced, disseminated or operated with the assistance of a **bot**?
4. Does the company **clearly disclose** how it enforces its **bot policy**?
5. Does the company **clearly disclose** data about the volume and nature of user **content** and **accounts restricted** for violating the company’s **bot policy**?
6. Does the company **clearly disclose** data about the volume and nature of **advertising content** and **accounts restricted** for violating the company’s **bot policy**?

⁷⁸ “Consultation Draft: Human Rights Risk Scenarios: Algorithms, Machine Learning and Automated Decision-Making,” *Ranking Digital Rights* (2019), https://rankingdigitalrights.org/wp-content/uploads/2019/07/Human-Rights-Risk-Scenarios_-_algorithms-machine-learning-automated-decision-making.pdf.

⁷⁹ Engler, A. (2020, January 22). The case for AI transparency requirements. Brookings Institution, <https://www.brookings.edu/research/the-case-for-ai-transparency-requirements/>, last accessed March 3, 2020.

7. Does the company clearly disclose that it removes **bots** from **engagement metrics** shown to users, such as sums of accounts that have taken a particular action?
8. Does the company regularly publish data about the total number of **bots** on the platform?

To see the full draft methodology, including a glossary of the above key terms highlighted in **bold**, see: “Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems,” *Ranking Digital Rights*, October 2019, <https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators-Targeted-advertising-algorithms.pdf>.

Key findings

Companies lack transparency about how they handle bots on their platforms, including their processes for ensuring that bots are not being used to artificially inflate messages or content.

Two of the three platforms evaluated for this indicator—**Facebook** and **Twitter**—disclosed some guidelines governing the use of bots on those platforms (F13, Element 2).⁸⁰ However, neither company defined what a bot is (F13, Element 1), nor did they explain how their bot policies are enforced (F13, Element 4) or whether they remove bots from engagement metrics (F13, Element 7).

For instance, **Facebook’s** “Platform Policy” provided the following guidelines: “Keep your app or bot’s description and categorization up-to-date;” “Ensure your bot is stable and functions properly;” “Your app or bot should not receive excessive negative feedback. Be sure your app insights reflect a positive experience.”⁸¹ But it disclosed no additional information beyond this about if and how it enforces these policies (F13, Element 4) or about removing bots from engagement metrics (F13, Element 7).

The use of bots on **Twitter** is governed by guidelines about the unacceptable use of automation on its platform.⁸² Rules include the following: “Don’t abuse the Twitter API or attempt to circumvent rate limits,” and “don’t spam or bother users, or otherwise send them unsolicited messages.” Twitter also publishes a transparency report on “platform manipulation,” defined by the company as “the use of Twitter to mislead others and/or disrupt their experience by engaging in bulk, aggressive, or deceptive activity. This activity includes, but is not limited to, spam, malicious automation (malicious use of bots),

⁸⁰ Three services—Facebook, Twitter, and YouTube (Google)—were piloted for F13.

⁸¹ “Platform Policy,” Facebook, <https://developers.facebook.com/policy/>, last accessed March 3, 2020.

⁸² “Automation rules,” Twitter, <https://help.twitter.com/en/rules-and-policies/twitter-automation>, last accessed March 3, 2020.

and inauthentic account abuse (fake accounts).⁸³ The report includes data on “anti-spam challenges,” used to describe the company’s process “for confirming whether a human is in control of an account we suspect is engaging in platform manipulation,” and spam reports. However, the data does not include the number of bots on the platform (F13, Element 8).

5.6 Informing and educating users about risks

Media, digital, and information literacy efforts are central to the protection and promotion of human rights.⁸⁴ For this reason, RDR developed a new draft indicator (F14) that calls on companies to advance digital literacy by educating users about the risks that advertising and algorithmic systems may pose to users’ online information ecosystems. In addition to publishing clear and transparent policies about how they use algorithms and about their ad targeting policies and practices, companies should also take extra steps to publish materials aimed at helping users understand the risks of these technologies on their fundamental freedom of expression and information rights.⁸⁵

The full text and elements for draft indicator F14 are displayed below, followed by key findings.

Draft Indicator F14: Informing and educating users about risks

The company should publish information to help users understand how **targeted advertising** and the use of **algorithms, machine learning and automated decision-making** influence their experience using the company’s products and services.

Elements:

1. Does the company publish practical materials that educate users on how to protect themselves from **advertisers’** attempts to mislead them?
2. Does the company publish practical materials that educate users on how to protect themselves from any potential undue psychological influence of the company’s use of **algorithms, machine learning and automated decision-making**?

⁸³ “Platform manipulation,” Twitter, <https://transparency.twitter.com/en/platform-manipulation.html>, last accessed March 3, 2020.

⁸⁴ “Addressing the impacts of Algorithms on Human Rights: Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems,” Council of Europe, Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence (2019), <https://rm.coe.int/draft-recommendation-of-the-committee-of-ministers-to-states-on-the-hu/168095eecf>.

⁸⁵ Standards advanced in this indicator are derived from: “Addressing the impacts of Algorithms on Human Rights: Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems,” Council of Europe, Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence (2019), <https://rm.coe.int/draft-recommendation-of-the-committee-of-ministers-to-states-on-the-hu/168095eecf>.

To see the full draft methodology, including a glossary of the above key terms highlighted in **bold**, see: “Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems,” *Ranking Digital Rights*, October 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-Targeted-advertising-algorithms.pdf.

Key findings

Companies do not make strong efforts to advance digital literacy by publishing practical materials that help educate users about the possible freedom of expression and information risks that could be caused by targeted advertising and algorithmic systems.

Beyond the policies evaluated in previous indicators, none of the companies published additional practical materials aimed at educating users on how to protect themselves from advertisers’ attempts to mislead them (F14, Element 1) or on how to protect themselves from any potential undue psychological influence of the company’s use of algorithms (F14, Element 2).⁸⁶

For instance, while **Facebook** disclosed some information about why users are seeing certain ads and how ad targeting works, the company did not disclose any practical materials that educate users on how to protect themselves from advertisers’ attempts to mislead them (F14, Element 1).⁸⁷ Similarly, **Deutsche Telekom Germany** disclosed materials addressing AI and ethics, including the ethical challenges that the development and use of AI can pose for citizens and society.⁸⁸ However, no disclosure could be located that provided clear guidance or examples of how users can protect themselves from harms that can result from the company’s use of algorithmic systems.

No companies published materials to help educate users about the potential psychological influence of algorithms (Element 2).

For a further discussion of our findings on this indicator, see **Section 7** which highlights the most challenging indicators and issues that arose during this pilot study.

⁸⁶ The following companies/services were piloted for this indicator: Apple (Group and Apple iOS); Deutsche Telekom (Group and Deutsche Telekom Germany, postpaid mobile); Facebook (Group and Facebook SNS); Google (Group, Google Search, Youtube, Android); Microsoft (Group, Bing and OneDrive); Telefónica Spain (postpaid mobile); Twitter (Group and Twitter SNS); and Vodafone (Group).

⁸⁷ “About Facebook Ads,” Facebook, <https://www.facebook.com/about/ads>, last accessed March 3, 2020.

⁸⁸ “Guidelines for Artificial Intelligence, Deutsche Telekom, <https://www.telekom.com/en/company/digital-responsibility/details/artificial-intelligence-ai-guideline-524366>, last accessed March 3, 2020.

6. Privacy

The Privacy category of the RDR Index evaluates whether a company's policies and commitments demonstrate concrete ways in which it respects the right to privacy of users, as articulated in the Universal Declaration of Human Rights,⁸⁹ the International Covenant on Civil and Political Rights,⁹⁰ and other international human rights instruments.⁹¹ The company's disclosed policies should demonstrate how it works to avoid contributing to actions that may interfere with users' privacy, except where such actions are lawful, proportionate, and for a justifiable purpose. Companies that perform well on these indicators demonstrate a strong public commitment to transparency not only in terms of how they respond to government and private requests for user information, but also how they determine, communicate, and enforce private rules and commercial practices that affect users' privacy.

The draft indicators published in October 2019 introduced a number of revisions to this category to include transparency and accountability standards for companies' targeted advertising policies and practices and for their development and use of algorithmic systems.⁹² Specifically, we expanded several existing Privacy category indicators (P1, P2) into "families" of indicators to include accessibility standards for companies' algorithmic system development policies.⁹³

We also expanded our "user information" indicators (Indicators P3 to P9, which examine company policies for handling user information) to address company disclosure of data inference policies and practices. We expanded Indicator P9—which evaluates how transparent companies are about data they collect about users through technical means, such as widgets and cookies—to include four new elements that aim to set transparency standards for the collection of user data through non-technical means, such as data-sharing agreements. We added two elements to existing Indicator P18, which calls on companies to inform and educate their users about the privacy risks stemming from the use of their services. These new elements examine companies' practices with respect to informing users about how they can protect themselves from the harmful effects of targeted advertising and the use of their data for the development and optimization of algorithmic systems.

The full list of new draft indicators in the Privacy category is presented in the box below, followed by a presentation of key findings.

⁸⁹ Universal Declaration of Human Rights, <https://www.un.org/en/universal-declaration-human-rights/>

⁹⁰ International Covenant on Civil and Political Rights, <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

⁹¹ Privacy category, *RDR 2019 Corporate Accountability Index*, <https://rankingdigitalrights.org/index2019/categories/privacy/>.

⁹² "Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems," *Ranking Digital Rights*, October 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-_Targeted-advertising-algorithms.pdf.

⁹³ Indicator P1: <https://rankingdigitalrights.org/index2019/indicators/p1/>; Indicator P2: <https://rankingdigitalrights.org/index2019/indicators/p2/>.

Privacy category—Draft indicators and elements on algorithms, targeted advertising**P1b:** Access to algorithmic system development policies**P2b:** Changes to algorithmic system development policies**P3b:** Inference of user information**P5, Elements 2 and 5:** Purpose for inferring user information**P7, Elements 3 and 4:** Users' control over their inferred information**P7, Elements 6 and 7:** Users' control over targeted advertising**P8, Element 5:** Users' access to their inferred information**P9, Elements 1 to 4:** Collection of user data by non-technical means**P18, Elements 2 and 3:** Inform and educate users about potential risks**P19:** Access to advertising metadata

To see the full draft methodology, including a full list of elements and a glossary of terms: "Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems," *Ranking Digital Rights*, October 2019,

https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-_Targeted-advertising-algorithms.pdf.

Key findings**Companies lack transparency about how they develop, share, and deploy the profiles of their users.**

- **Companies lack transparency about how they develop and train algorithmic systems.** No company published a discrete policy with guidelines for how they develop algorithmic systems (see *Section 6.1 below*).
- **Companies lack transparency about their data inference policies and practices.** Although slightly more than half of the piloted companies disclosed at least some information regarding what types of user information they infer and how they do so, just one (**Telefónica**) gave users any option to control whether their information is inferred in the first place (see *Section 6.2 below*).
- **Companies disclose little about options users have to control targeted advertising and how their information is used to develop and train algorithmic systems.** No company clearly stated whether targeted advertising is on or off by default. Only one company (**Telefónica**) provided users with options

on how to control the use of their information for the development of algorithmic systems (see Section 6.3 below).

- **Companies lack transparency about whether or how they acquire user information through non-technical means**, such as through contractual agreements with data brokers. Only one company (Microsoft) disclosed information about these types of data acquisition practices, but even that information was limited (see Section 6.4 below).
- **Most companies take no extra steps to educate users about the privacy risks related to targeted advertising and algorithmic systems**. Just two companies—**Apple** and **Facebook**—published materials about privacy risks related to targeted advertising. No company published any materials about risks to privacy in relation to the development of algorithmic systems (see Section 6.5 below).
- Most companies disclosed nothing about if and how users can access their advertising metadata (see more in Section 6.6 below).

6.1 Algorithmic system development policies

The development and testing of algorithmic systems can pose significant risks to privacy, particularly when companies use user information to develop, train, and test these systems without the data subject’s informed consent.⁹⁴ Therefore, just as companies should clearly disclose their policies for using algorithmic systems (see draft Indicator F1d, F2d), companies should also clearly disclose terms that outline how they develop and test algorithmic systems.⁹⁵ These policies should be easy to find and understand (P1b), and companies should commit to notify users when their algorithmic development policies change (P2b). Companies should disclose this information so that users can understand how their information is being used, and whether to use a company’s products and services.⁹⁶

The full text for draft indicators P1b and P2b are displayed below, followed by key findings on these indicators.

⁹⁴ Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY, USA: PublicAffairs.

⁹⁵ RDR defines “algorithmic system development policies” as policies that outline a company’s practices and standards related to the development and testing of algorithms, machine learning and automated decision-making. See glossary of terms: “Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems,” *Ranking Digital Rights*, October 2019, https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-_Targeted-advertising-algorithms.pdf.

⁹⁶ “Addressing the impacts of Algorithms on Human Rights: Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems,” Council of Europe, Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence (2019), <https://rm.coe.int/draft-recommendation-of-the-committee-of-ministers-to-states-on-the-hu/168095eecf>.

Draft indicators—algorithmic system development policies

P1(b). Access to algorithmic system development policies: The company should offer **algorithmic system development policies** that are easy to find and easy to understand.

P2(b). Changes to algorithmic system development policies: The company should **clearly disclose** that it provides notice and documentation to users when it changes its **algorithmic system development policies**.

To see the full draft methodology, including a glossary of the above key terms highlighted in **bold**, see: “Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems,” *Ranking Digital Rights*, October 2019,

https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-_Targeted-advertising-algorithms.pdf.

Key findings

While every company in this pilot deploys algorithms in various ways in its products and services, none disclosed a discrete policy governing how they develop and train these systems.⁹⁷ Similar to our findings for algorithmic use policies (F1d, F2d), some companies had limited disclosure of how they use algorithmic systems but none disclosed a discrete policy that clearly and prominently describes their policies for developing these systems.

- **Facebook** disclosed that its “systems automatically process content and communications” but disclosed nothing about its development of algorithmic systems.⁹⁸
- **Microsoft** disclosed how user information is processed by algorithmic systems, but it did not disclose a clear policy describing how these systems are developed.⁹⁹
- **Vodafone UK** disclosed that it uses “big data analytics”—which it defines as “mathematically driven analysis techniques on large and varied data sets (that is why it is ‘big’ data) to uncover hidden patterns and hitherto unrevealed trends”—but offered no clear policy or terms explaining how it develops and trains these systems.¹⁰⁰

⁹⁷ Companies/services piloted on these indicators: Apple (iOS), Google (Search, YouTube, Android), Facebook (Facebook), Microsoft (Bing, OneDrive), Twitter (Twitter), Deutsche Telekom Germany (postpaid mobile), Telefónica Spain (postpaid mobile), Vodafone UK (postpaid mobile).

⁹⁸ “Data Policy,” Facebook, <https://www.facebook.com/about/privacy>, last accessed March 3, 2020.

⁹⁹ “Privacy Statement,” Microsoft, <https://privacy.microsoft.com/en-us/privacystatement>, last accessed March 3, 2020.

¹⁰⁰ “Privacy Policy,” Vodafone UK, <https://www.vodafone.co.uk/privacy#/privacy-policy>, last accessed March 3, 2020.

For a further discussion of our findings on these indicators, see **Section 7** which highlights the most challenging indicators and issues that arose during this pilot study.

6.2 Data inference policies

In addition to collecting information about users, companies also perform big data analytics to infer additional data points on the basis of the collected information. Big data analytics use algorithmic decision-making systems to make “non-intuitive and unverifiable inferences and predictions about the behaviors, preferences, and private lives of individuals” in a way that may be discriminatory and biased.¹⁰¹ These practices are often privacy-invasive and unverified, but can significantly impact on our “private lives, identity, reputation, and self-determination.”¹⁰²

The RDR Index has an existing set of indicators (P3 to P9) evaluating how transparent companies are about what type of user information they collect, share, for what purposes, and about options users have to control their own information.¹⁰³ In addition to being fully transparent about these policies and practices, companies should also clearly disclose their data inference policies—including what types of data they infer, how and for what purpose (P3b), and give users options to control what is inferred about them (P7, Elements 3 and 4). Companies should also enable users to obtain all of the data that has been inferred about them (P8, E5).

The full text for draft indicators and elements addressing company disclosure of their data inference policies is displayed below, followed by key findings on these indicators and elements.

Pilot indicators and elements addressing company transparency of data inference policies and practices

P3b, Element 1: Does the company **clearly disclose** all the types of **user information** it infers on the basis of collected user information?

¹⁰¹ Wachter, Sandra and Mittelstadt, Brent, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI (October 5, 2018). Columbia Business Law Review, 2019(2), <https://ssrn.com/abstract=3248829>.

¹⁰² Sandra Wachter and Brent Mittelstadt, “A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI,” *Oxford Business Law Blog*, October 2018, <https://www.law.ox.ac.uk/business-law-blog/blog/2018/10/right-reasonable-inferences-re-thinking-data-protection-law-age-big>.

¹⁰³ See our findings on these indicators from the 2019 RDR Index: <https://rankingdigitalrights.org/index2019/report/privacy/#section-52>.

P3b, Element 2: For each type of **user information** the company infers, does the company **clearly disclose** how it infers that user information?

P3b, Element 3: Does the company **clearly disclose** that it limits inference of user information to what is directly relevant and necessary to accomplish the purpose of its service?

P5, Element 2: For each type of user information the company infers, does the company **clearly disclose** its purpose for the inference?

P5, Element 5: Does the company **clearly disclose** that it limits its use of user information to the purpose for which it was collected or inferred?

P7, Element 3: For each type of user information the company infers on the basis of collected information, does the company **clearly disclose** whether users can control if the company can attempt to infer this user information?

P7, Element 4: For each type of user information the company infers on the basis of collected information, does the company **clearly disclose** whether users can delete this user information?

P8, Element 5: Does the company **clearly disclose** that users can obtain all the information that a company has inferred about them?

To see full draft methodology, including glossary of above key terms highlighted in **bold**: “Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems,” *Ranking Digital Rights*, October 2019, [https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators - Targeted-advertising-algorithms.pdf](https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators-Targeted-advertising-algorithms.pdf).

Key findings

Companies lack clear disclosure of their data inference policies and practices, and few give users any options to control what data is used to make inferences about them.¹⁰⁴ While just more than half of the eight companies evaluated on these elements did disclose that they make inferences from some of the user information that they collect, they did not provide much additional information about their inference policies or practices beyond this, including the purpose for inferring user information or what options users have to control what is inferred. No company evaluated disclosed options for users to obtain the information a company has inferred about them.

- Five companies of the eight companies evaluated on these elements—**Google, Microsoft, Telefónica Spain, Twitter, Vodafone UK**—gave some information about what user data they infer and how they do so (P3b, Element 1 and Element 2).

¹⁰⁴ For these indicators/elements, we piloted the following companies/services: Apple (iOS); Google (Search, YouTube, Android); Facebook (the social networking service); Microsoft (Bing, OneDrive); Twitter (the social networking service); Deutsche Telekom Germany (postpaid mobile); Telefónica Spain (postpaid mobile), and Vodafone UK (postpaid mobile).

- Only two companies—**Microsoft** and **Telefónica Spain**—disclosed options for users to delete some of the information inferred about them (P7, Element 4). In the case of Microsoft, this capability was limited to inferred location data.¹⁰⁵ No other company—including **Apple**, **Google**, **Facebook**, or **Twitter**—disclosed options for users to control or delete the information that these companies infer about them (P7, Element 3 and 4).
- Three companies—**Microsoft**, **Telefónica Spain**, and **Twitter**—disclosed some information about their purpose for inferring user information (P5, Element 2). Three companies—**Google**, **Telefónica Spain**, and **Deutsche Telekom Germany**—disclosed a commitment to limit the use of collected or inferred user data to the purpose for which it was collected or inferred (P5, Element 5). **Telefónica Spain** was the only company to commit only to infer user information that was directly relevant and necessary to accomplish the purpose of the provided service (P3b, Element 3).¹⁰⁶
- No company disclosed any options for users to obtain a copy of the information it inferred about them (P8, Element 5).

6.3 User control

Indicator P7 in the RDR Index evaluates whether companies clearly disclose options allowing users to control what information the company collects and retains, and how it is used.¹⁰⁷ Our draft methodology expands this indicator to encompass users' ability to control whether targeted advertising is displayed and how their information is used to develop algorithmic systems.

While it is important for companies to be transparent about how their targeted advertising systems work, users may be unaware that they are being targeted in the first place. Draft Elements 6 and 7 assess whether the company discloses the default setting for the display of targeted advertising, and whether the default option for targeted advertising is off, respectively. Similarly, companies may use the information that they collect and infer about users to develop, optimize and train algorithmic systems (including ad targeting systems) without explicitly stating that they do so. New Elements 8 and 9 for this indicator pertain to the practice of using user information (both collected and inferred) for the development of algorithmic systems.

Draft elements added to Indicator P7 are displayed below, followed by key findings on these elements.

¹⁰⁵ "Privacy Statement," Microsoft, <https://privacy.microsoft.com/en-us/privacystatement>, last accessed March 3, 2020.

¹⁰⁶ "Movistar Privacy Policy," Telefónica Spain, <http://www.movistar.es/estaticos/politica-privacidad.pdf>, last accessed March 3, 2020.

¹⁰⁷ See our findings on P7 from the 2019 RDR Index: <https://rankingdigitalrights.org/index2019/report/privacy/#section-53>.

P7. Users' control over their own user information

The company should **clearly disclose** to users what **options they have to control** the company's **collection, inference, retention** and use of their **user information**.

Draft Elements:

Element 6: Does the company **clearly disclose** whether the display of **targeted advertising** is on or off by default?

Element 7: Does the company **clearly disclose** that users can opt in to being shown **targeted advertising**?

Element 8: Does the company **clearly disclose** that it provides **users** with options to control how their **user information** is used for the development of **algorithmic systems**?

Element 9: Does the company **clearly disclose** whether it uses **user information** to develop **algorithmic systems** by default, or not?

For the full draft methodology, including glossary of the above key terms highlighted in **bold**, see: "Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems," *Ranking Digital Rights*, October 2019, <https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators--Targeted-advertising-algorithms.pdf>.

Key findings

Companies do not give users clear options to control targeted advertising or whether their information is automatically used to develop and train algorithmic systems.

- No company clearly stated the default settings for targeted advertising (P7, Element 6). For most companies, the default settings could be deduced from their disclosure, but no company clearly disclosed the targeted advertising default settings. For instance, **Facebook** disclosed that "there is no way to hide all ads"—which indicates targeted advertising is *on* by default, and that users cannot completely opt out of receiving targeted advertising.¹⁰⁸
- No company disclosed that users can opt in to being shown targeted advertising (P7, Element 7).
- Only one company—**Telefónica Spain**—provided options for users to control how their information is used for the development of algorithmic systems (P7, Element 8).

¹⁰⁸ "Control the ads you see," Facebook, https://www.facebook.com/help/1075880512458213/?helpref=hc_fnav, last accessed March 3, 2020.

- None of the companies evaluated disclosed whether they use user information to develop algorithmic systems by default (P7, Element 9).

6.4 Collection of user information by non-technical means

Indicator P9 of the RDR Index evaluates whether companies disclose if they track users across the internet through technical means, such as by using cookies, plug-ins, and widgets.¹⁰⁹ Company disclosure of these practices helps users understand if and how their activities are being tracked by companies even when they are not on a host company's website or are a user of a particular service or platform. However, this is not the only way that companies acquire user information from third parties. Companies can also acquire user information through non-technical means, including as part of a contractual agreement, and this acquired data can become part of a "digital dossier" that companies may hold on its users, which can then form the basis for inferred and shared user information.

Therefore, we added four new elements to Indicator P9, which apply the same transparency standards to companies that acquire data about users through non-technical means, such as through purchases, data-sharing agreements, and other contractual relationships with third parties. We expect companies to clearly disclose what user information they collect from third parties through non-technical means (P9, Element 1), how it collects this information (P9, Element 2), its purpose for doing so (P9, Element 3), and how long it retains this user information (P9, Element 4).

Draft elements added to Indicator P9 are displayed below, followed by key findings on these elements.

Indicator P9. Collection of user information from third parties

The company should **clearly disclose** its practices with regard to **user information** it **collects** from third-party websites or **apps**, including through technical means.

Draft Elements 1 to 4:

Element 1: Does the company **clearly disclose** what **user information** it collects from **third parties** through **non-technical means**?

Element 2: Does the company **clearly disclose** how it collects **user information** from **third parties** through **non-technical means**?

Element 3: Does the company **clearly disclose** its purpose for collecting **user information** from **third parties** through **non-technical means**?

Element 4: Does the company **clearly disclose** how long it retains the **user information** it collects from **third parties** through **non-technical means**?

¹⁰⁹ See Indicator P9: <https://rankingdigitalrights.org/index2019/indicators/p9/>.

For the full draft methodology, including glossary of the above key terms highlighted in **bold**, see: “Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems,” *Ranking Digital Rights*, October 2019, <https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators-Targeted-advertising-algorithms.pdf>.

Key findings

Companies lack transparency about whether and how they obtain user information through “non-technical” means, such as through contractual agreements or data brokers.¹¹⁰

Only one company—**Microsoft**—disclosed that it obtains data from third parties through non-technical means, but even this information was not comprehensive (P9, Element 1). For instance, it did not disclose how this data is collected (P9, Element 2) or for how long it is retained (P9, Element 4).

Note that while RDR only piloted this indicator for internet and mobile ecosystem companies, we are considering applying it to telecommunications companies since they also can acquire user data through contractual agreements.

6.5 Inform and educate users about risks

Media, digital, and information literacy efforts are central to the protection and promotion of human rights, particularly in the context of algorithmic systems.¹¹¹ For this reason, we added two draft elements to the existing Indicator P18 to assess company efforts to increase user education about the privacy risks associated with targeted advertising and algorithmic systems (Element 2 and 3).

Draft elements added to Indicator P18 are displayed below, followed by key findings on these elements.

Indicator P18. Inform and educate users about potential risks

Draft elements:

Element 2: Does the company publish practical materials that educate **users** on how to protect themselves from the privacy risks associated with the company’s **targeted advertising** practices?

¹¹⁰ The following companies/services were piloted for these elements: Apple (iOS); Google (Search, YouTube, Android); Facebook (Facebook social networking service); Microsoft (Bing, OneDrive); Twitter (Twitter social networking service).

¹¹¹ “Addressing the impacts of Algorithms on Human Rights: Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems,” Council of Europe, Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence (2019), <https://rm.coe.int/draft-recommendation-of-the-committee-of-ministers-to-states-on-the-hu/168095eecf>.

Element 3: Does the company publish practical materials that educate **users** on how to protect themselves from the privacy risks associated with the inclusion of their **user information** in the development and optimization of **algorithmic systems**?

For the full draft methodology, including a glossary of the above key terms highlighted in **bold**, see: “Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems,” *Ranking Digital Rights*, October 2019, <https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators -Targeted-advertising-algorithms.pdf>.

Key findings

Companies do not make strong efforts to advance digital literacy by publishing educational materials about potential privacy risks related to targeted advertising or algorithmic systems.¹¹²

As previous RDR Index research has shown, all of the eight companies included in this pilot publish materials to educate users on how to protect themselves from cybersecurity risks relevant to their products or services (P18).¹¹³ But only two of these eight companies—**Apple** and **Facebook**—publish materials aimed at educating users on how to protect themselves from the privacy risks associated with the company’s targeted advertising (P18, Element 2). No companies published materials to educate users on how to protect themselves from the privacy risks associated with algorithmic system development (P18, Element 3).

Apple’s Manage Your Privacy page provides comprehensive information on how users can protect themselves from the privacy risks associated with the company’s targeted advertising practices.¹¹⁴ The policy states: “Advertising is a source of income for some app developers. To help protect your privacy, we have developed the nonpersistent Advertising Identifier. This requires all ads in every one of our apps to clearly indicate that they are advertisements, and to provide specific information on why they were delivered to you at that moment. Advertisers use the Advertising Identifier to control the number of times you see a given ad, to measure the effectiveness of ad campaigns, and, unless you choose to opt out, to serve you more relevant ads. When you enable Limit Ad Tracking, your Advertising Identifier cannot be used by third-party apps to serve you targeted ads. Apple’s advertising service won’t serve interest-based ads to children under 13 and Managed Apple IDs.”

¹¹² The following companies / services were piloted for this indicator: Apple (iOS); Deutsche Telekom Germany (postpaid mobile); Facebook (the social networking service); Google (Search, YouTube, Android); Microsoft (Bing, OneDrive); Telefónica Spain (post paid mobile); Twitter (the social networking service); and Vodafone UK (postpaid mobile).

¹¹³ See P18 data from 2019 RDR Index: <https://rankingdigitalrights.org/index2019/indicators/p18/>.

¹¹⁴ “Manage your privacy,” Apple, <https://www.apple.com/privacy/manage-your-privacy/>, last accessed March 9 2020.

Facebook provides some tips on how users can protect themselves from adware¹¹⁵ and how parents can adjust their children's ads privacy settings.¹¹⁶ But it provides no information on the risks associated with its targeted advertising policies and practices such as (potential) misuse of data by third parties and how users can take steps to protect themselves from such risks.

6.6 User access to advertising targeting metadata

While some companies have started to provide information to users about why particular advertising content is shown to them, this practice is far from universal and appears to be limited to on-platform advertising only (as opposed to targeted advertising that appears on third-party websites through an advertising network). This new indicator calls on companies to clearly explain—in a manner that is accessible without creating a user account—how users can access detailed information on all the targeted advertising that the company shows them (both on- and off-platform, as the case may be for each company).

In order to target ads, companies typically assign each user to any number of audience categories (Facebook, for instance, calls them “affinity groups”). Advertisers can then select which audience categories they want to target. Users should be able to know which audience categories the company has assigned them to, on the basis of information that the company has collected or inferred about users (Element 1). In addition to knowing which audience categories they have been assigned to, users should be able to know which audience categories each ad they see has been targeted to, for both on-platform ads (Element 2) and off-platform ads (Element 4). Users should also be able to access a full list of all the advertisers who have attempted to influence them through on-platform targeted advertising (Element 3) and off-platform targeted advertising (Element 5). Full disclosure on these elements would enable users to know why they are seeing each ad that they see while using a company’s services and around the internet.

The full text and elements of draft Indicator P19 are displayed below, followed by key findings on this indicator.

Draft Indicator P19. User access to advertising targeting metadata

The company should **clearly disclose** how **users** can access key information about the **targeted advertising** that they see.

Elements:

1. Does the company **clearly disclose** how **users** can access the list of **advertising audience categories** to which the company has assigned them?
2. Does the company **clearly disclose** how **users** can access the list of **advertising audience categories** to which each piece of **advertising content** they see while using the product or service was targeted?

¹¹⁵“ Adware,” Facebook, <https://www.facebook.com/help/380632641992051>, last accessed March 9 2020.

¹¹⁶“Control the Ads You See,” Facebook, https://www.facebook.com/help/1075880512458213/?helpref=hc_fnav, last accessed March 9 2020.

3. Does the company **clearly disclose** how **users** can access the list of **advertisers** who have attempted to influence them through the company's on-platform **targeted advertising** technologies?
4. Does the company **clearly disclose** how **users** can access the list of **advertising audience categories** to which each piece of **advertising content** they see off-platform was targeted through the company's **advertising network**?
5. Does the company **clearly disclose** how **users** can access the list of **advertisers** who have attempted to influence them through the company's off-platform **advertising network**?

For the full draft methodology, including a glossary of the above key terms highlighted in **bold**, see: "Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems," *Ranking Digital Rights*, October 2019, <https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators-Targeted-advertising-algorithms.pdf>.

Key findings

Companies lacked transparency about whether and how users can access key information and metadata used by advertisers to target them with interest-based ads.¹¹⁷

With the exception of **Google**, no company disclosed information about how users can access the advertising audience categories to which each user is assigned (Element 1, Element 2, Element 4). Google disclosed a minimal amount of information on the targeting categories that are applied to users (Element 1). None of the evaluated companies provided access to a comprehensive list of these categories and none reported information about how to obtain the targeting categories associated with each piece of advertising content a user was shown (Element 2). No company disclosed how users can obtain a list of the advertisers who attempted to target them (Element 3, Element 5).

Transparency was also weak in the case of off-platform advertising. While companies routinely rely on their advertising network to show users promoted content off-platform based on a set of advertising categories, none disclosed anything about the categories themselves (Element 4) or the advertisers involved (Element 5).

¹¹⁷ The following companies / services were piloted for this indicator: Apple (iOS); Deutsche Telekom Germany (postpaid mobile); Facebook (the social networking service); Google (Search, YouTube, Android); Microsoft (Bing, OneDrive); Telefónica Spain (post paid mobile); Twitter (the social networking service); and Vodafone UK (postpaid mobile).

7. Most challenging indicators and issues

In this section, we present some of the more challenging indicators and issues we encountered during the research, which raised methodological questions we plan to address during the next phase of our methodology work.

7.1 Algorithmic system use and development policies

None of the eight companies evaluated in the pilot disclosed policies outlining their use (F1d) or development (P1b) of algorithmic systems (see Sections 5.3 and 6.1 above). This raised some methodological questions about how we are defining these policies and what we are looking for companies to disclose.

Note that we developed these indicators in consultation with numerous stakeholders and based on evolving standards of algorithmic transparency for both the public and private sector. For instance, the Council of Europe recommends that companies that use algorithmic systems which can trigger significant human rights impacts should ensure that they publish a clear policy summarizing the nature and functions of these systems and how they are developed: “Terms of service should be reasonably concise, easily understandable and contain clear and succinct language about possibilities for users to manage settings.”¹¹⁸

Pilot research showed that no company published a discrete policy describing how algorithms are developed and used. Some companies published information about how they deploy algorithms in different functions (like the Facebook News Feed) but no company published a standalone algorithm “terms of service” policy in alignment with emerging standards advocated by some experts. Given the lack of disclosure on these indicators, RDR plans to further investigate these standards through continued research and stakeholder engagement as we finalize the 2020 RDR Index methodology.

7.2 Bot policies

Two of the three platforms evaluated for this indicator disclosed some guidelines governing the use of bots on those platforms (F13, Element 2). However, none of the companies defined what a bot is (F13, Element 1), nor did they explain how their bot policies are enforced (F13, Element 4) or whether they remove bots from engagement metrics (F13, Element 7).

One of the challenges researchers faced was to determine the scope of this indicator. Whether bots are allowed and how they are used is different from one platform to another and this created some challenges for researchers to evaluate companies. There are

¹¹⁸ “Addressing the impacts of Algorithms on Human Rights: Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems,” Council of Europe, Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence (2019), <https://rm.coe.int/draft-recommendation-of-the-committee-of-ministers-to-states-on-the-hu/168095eecf>.

services that allow the use of bots by businesses, but that does not necessarily mean that companies allow these to generate and disseminate content (F13, Element 2 and Element 3).

The bot indicator also raised security questions. While RDR advocates for transparency, we also acknowledge cases when security factors play a bigger role. During the public consultation, security experts pointed out that asking companies to disclose their definition of bots (F13, Element 1) might undermine their efforts to enforce their bot policies and that, by telling users how companies define bots, they enable them to circumvent their bot policies. RDR will consider this and other factors when deciding about whether to include this indicator in the final 2020 RDR Index methodology.

7.3 Access to advertising metadata

Of the eight piloted companies, only Google disclosed any information about how its users can access key information about the targeted advertising that they see (P19). However, even this information was limited: it only revealed how users can access the list of advertising audience categories to which they were assigned, but did not reveal any other information (see P19 analysis).

The lack of disclosure from companies raised some methodological questions about how to assess companies' transparency around advertising metadata. The RDR Index methodology evaluates only publicly available policies; we do this because users should have the opportunity to review a company's policies and practices prior to their joining a service or platform. Although disclosure on this indicator was very low, RDR believes companies should be disclosing their policies for providing users access to their advertising metadata—whether or not a user joins a platform or service. We will continue to research this indicator and our findings on it as we draft the 2020 RDR Index methodology.

8. Conclusions and next steps

Results of this pilot will be further analyzed by the RDR research team, taking into account feedback we receive from stakeholders. In early April 2020, we plan to publish a full draft of the 2020 RDR Index methodology, which will incorporate indicators on targeted advertising and algorithms piloted in this study, as well as add new companies and services. The draft 2020 RDR Index methodology will also include some revisions to the existing methodology.

The publication of the draft 2020 RDR Index methodology will be followed by another period of public consultation. During this period of stakeholder engagement, RDR will address more specific issues we encountered during this pilot as we make decisions about how to incorporate new indicators and companies into the broader RDR Index.

We plan to finalize the 2020 RDR Index methodology in May 2020. Results of the 2020 RDR Index will be published in February 2021.

We welcome input or feedback about research presented in this study or the methodology at methodology@rankingdigitalrights.org.

9. Glossary of key terms

The following is a short list of select key terms referenced in this study.

For the the full glossary of terms on these draft indicators, see: “Draft Indicators: Transparency and accountability standards for targeted advertising and algorithmic decision-making systems,” *Ranking Digital Rights*, October 2019, at: https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-_Targeted-advertising-algorithms.pdf.

Algorithms — An algorithm is a set of instructions used to process information and deliver an output based on the instructions’ stipulations. Algorithms can be simple pieces of code but they can also be incredibly complex, “encoding for thousands of variables across millions of data points.” In the context of digital platforms and telecommunications companies, some algorithms—because of their complexity, the amounts and types of user information fed into them, and the decision-making function they serve—have significant implications for users’ human rights, including freedom of expression and privacy. See more at: “Algorithmic Accountability: A Primer,” Data & Society: https://datasociety.net/wp-content/uploads/2018/04/Data_Society_Algorithmic_Accountability_Primer_FINAL-4.pdf.

Algorithmic system — A system that uses algorithms, machine learning and/or related technologies to automate, optimize and/or personalize decision-making processes.

Artificial intelligence — Artificial intelligence has an array of uses and meanings. For the purposes of RDR’s methodology, artificial intelligence refers to systems that resemble, carry out, or mimic functions that are typically thought of as requiring intelligence. Examples include facial recognition software, natural language processing, and others, the use of which by internet, mobile, and telecommunications companies have implications for people’s freedom of expression and privacy rights. See: “Privacy and Freedom of Expression in the Age of Artificial Intelligence,” <https://privacyinternational.org/sites/default/files/2018-04/Privacy%20and%20Freedom%20of%20Expression%20%20In%20the%20Age%20of%20Artificial%20Intelligence.pdf>.

Automated decision-making — Technology that makes decisions without significant human oversight or input in the decision-making process, such as through the use of artificial intelligence or algorithms.

Data inference — Companies are able to draw inferences and predictions about the behaviors, preferences, and private lives of its users by applying “big data” analytics and algorithmic decision making technologies. These methods might be used to make inferences about user preferences or attributes (e.g., race, gender, sexual orientation), and opinions (e.g., political stances), or to predict behaviors (e.g., to serve advertisements). Without sufficient transparency and user control over data inference, privacy-invasive and non-verifiable inferences cannot be predicted, understood, or refuted by users. *For more see:* Wachter, Sandra and Mittelstadt, Brent, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI (October 5, 2018). Columbia Business Law Review, 2019(2), <https://ssrn.com/abstract=3248829>.

Targeted advertising — Targeted advertising, also known as “interest-based advertising,” “personalized advertising,” or “programmatic advertising,” refers to the practice of delivering tailored ads to users based on their browsing history, location information, social media profiles and activities, as well as demographic characteristics and other features. Targeted advertising relies on vast data collection practices, which can involve tracking users’ activities across the internet using cookies, widgets, and other tracking tools, in order to create detailed user profiles.

Targeting parameters — The conditions, typically set by the advertiser, that determine which users will be shown the advertising content in question. This can include users’ demographics, location, behavior, interests, connections, and other user information